

Margaret M. Vierbuchen
Wyoming State Bar No. 8-6767
Assistant United States Attorney
United States Attorney's Office for the District of Wyoming
P.O. Box 668
Cheyenne, WY 82003
(307) 772-2124
Margaret.Vierbuchen3@usdoj.gov

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF WYOMING

UNITED STATES OF AMERICA,

Plaintiff,

v.

PETER SZANTO,

Defendant.

Case No. 23-CR-95-SWS

**Government's Response in Opposition to Defendant's Motion to Suppress Data Obtained
from Defendant's Internet Accounts**

Defendant Peter Szanto seeks to suppress "all evidence from the contents of Defendant's Internet accounts from Google, and T-Mobile, as a fruit of its unlawful seizure of these materials in violation of the Fourth Amendment." (ECF No. 88.) As outlined below, this Court should deny the Defendant's motion because it is without basis in fact and law.

I. Background

A. Procedural Background

On July 19, 2023, an *Indictment* was returned by a District of Wyoming grand jury, charging the Defendant with one count of making a false statement in a bankruptcy proceeding, in violation of 18 U.S.C. § 152(2); a bankruptcy fraud scheme, in violation of 18 U.S.C. § 157; and

falsification of records in a bankruptcy, in violation of 18 U.S.C. § 1519. (ECF No. 1.) In short, it is alleged that after defaulting in 2009 on his Loan with JP Morgan Chase—a Loan secured by his Newport Beach, California home—the Defendant engaged in a nine-year scheme to hinder and delay the lawful foreclosure of his home by initiating bankruptcy proceedings (to trigger the automatic stay) in five different jurisdictions, including Wyoming. (*See id.* (Count 2).) Further, the *Indictment* alleges the Defendant falsified records submitted in the bankruptcy proceeding and gave false testimony under oath at a Creditors’ Meeting. (*See id.* (Counts 1 and 3).)

On August 8, 2023, Special Agents of the Federal Bureau of Investigation (“FBI”) arrested the Defendant at his Newport Beach home. (ECF No. 11.) On August 9, 2023, the Defendant was released on an unsecured appearance bond of \$25,000.00, with pre-trial release contingent upon certain conditions, including GPS monitoring. (ECF No. 17.) Trial is currently set for April 1, 2024. (ECF No. 63.)

B. Factual Background

The Defendant moves to suppress records obtained from Google and T-Mobile as it relates to two court *Orders* obtained pursuant to 18 U.S.C. 2703(d) and alleged “preservation requests.” The relevant facts relating to the Defendant’s motion are outlined below.

1. Google Records

On October 5, 2022, FBI Special Agent Amanda Fritz sent a preservation letter to Google for three Gmail accounts. (*See* Bates No. 3223 (¶29) [Search Warrant Affidavit of Special Agent Fritz].) The next day, October 6, 2022, the United States submitted an *Application* for a 18 U.S.C. § 2703(d) order to U.S. Magistrate Judge Kelly H. Rankin. (Ex. 1 (Bates No. 25240–45); *see also*

Bates No. 605–06 [FBI 302 documenting Google response]).¹ The United States provided the following specific and articulable facts in support of its *Application*:

On July 12, 2022, Probate Estate of Susan Szanto (the “Debtor”), a Wyoming corporation, filed a chapter 11 bankruptcy petition (the “Petition”) in the United States Bankruptcy Court for the District of Wyoming. The Petition was completed, signed, and authorized to be filed by Peter Szanto, the husband of the late Susan Szanto. At all relevant times, Mr. and Mrs. Szanto have resided in California. Mr. Szanto’s owns two residences in California, one of which is located at 11 Shore Pine Dr., Newport Beach, CA, 92657 (the “Newport Beach Property”), with an estimated valued of at least \$4,500,000. Ex. 1 at para. 5.

Mr. Szanto is well known to the federal court system, as well as state court system, having been found by courts to be a serial and vexatious litigant. Mr. Szanto has filed bankruptcy filings in the Central District of California in 2013 (where the Newport Beach Property is located), in the District of Nevada in 2013, in the District of Oregon in 2016, in the Southern District of California (SDCA) in June 2022, and, most recently, in the District of Wyoming in July 2022. As a general matter, the commencement of a bankruptcy case invokes the automatic stay of § 362(a) of the Bankruptcy Code which prohibits certain creditors from collecting debts until further Court order. *Id.* at para. 6.

Of particular note, on July 21, 2022, less than two months after filing a *pro se* bankruptcy petition in the SDCA, U.S. Bankruptcy Chief Judge Christopher B. Latham lifted the automatic stay due to Debtor Peter Szanto’s “bad faith” and found that “Debtor Peter Szanto has engaged in a scheme to delay and hinder [JP Morgan Chase’s] efforts to foreclose” on the Newport Beach Property. On July 22, 2022, Judge Latham issued an Order dismissing the case for improper venue. Mr. Szanto’s *pro se* appeal of this dismissal is pending. *Id.* at para. 7.

The Debtor’s bankruptcy filing in Wyoming on July 12, 2022, as well as his bankruptcy filings in other bankruptcy courts and state court filings, is believed to be an attempt by Mr. Szanto to continue his scheme to hinder and delay foreclosure on the Newport Beach Property which has been his residence over the years. Mr. Szanto defaulted on his loan from JP Morgan Chase Bank over thirteen (13) years ago, his default remains uncured, and he owes more than \$2 million on the loan secured by the Newport Beach Property. *Id.* at para. 8.

As part of a possible scheme to hinder and delay foreclosure on the Newport Beach Property, the Debtor was recently formed in Wyoming on May 22, 2022, which was less than two months prior to Debtor’s bankruptcy filing in Wyoming on July 12, 2022. It is suspected that the Debtor is effectively a shell company with

¹ Though initially sealed, the 2703(d) Applications and Orders referenced herein have been unsealed.

the Debtor's only asset being an interest in the Newport Beach Property. *Id.* at para. 19.

Regarding the incorporation of the Debtor, at a creditor's meeting on August 16, 2022, Mr. Szanto testified that unbeknownst to him, Miriam Jabotinski, a long-time friend of his late wife, incorporated the Debtor in Wyoming to preserve mineral interests his wife and Ms. Jabotinski uncovered while prospecting in Wyoming (of which he was unaware until very recently). Wyoming Secretary of State Records reveal that at 3:44 a.m. on May 22, 2022, a person purporting to be Miriam Jabotinski made an online filing with the Wyoming Secretary of State. This filing consisted of the Articles of Incorporation of the Debtor and listed the principal and mailing address of the Debtor as the Newport Beach Property. The filing further identified Ms. Jabotinski as the incorporator and "CEO" with a contact Gmail address of **miriamjabotinski@gmail.com**. *Id.* at para. 10.

During the Wyoming bankruptcy proceeding, it was represented that on May 31, 2022, Ms. Jabotinsky, using the Gmail address stated in Attachment **miriamjabotinski@gmail.com**, emailed Mr. Szanto, at the Gmail address stated in Attachment **szanto.pp@gmail.com**, informing him that she had incorporated the Debtor and "hereby appoints Peter Szanto as manager, director and Operations Officer for the continued protection and expansion of The Estate of Susan Szanto." Although Mr. Szanto testified that Ms. Jabotinski acted without his knowledge, also on May 31, 2022, in his capacity as the executor of his late wife's estate, Mr. Szanto signed a "California Grant Deed" transferring a 50% undivided interest in the Newport Beach Property to the Debtor. At this time, it is unknown if Ms. Jabotinski is in fact a real person, but it is suspected that the Wyoming bankruptcy filing and the Wyoming incorporation of the Debtor was another scheme perpetrated by Mr. Szanto to forestall the lawful foreclosure of his Newport Beach Property. The U.S. District Court of Wyoming dismissed the Debtor's Petition on August 17, 2022. *Id.* at para. 11.

On October 6, 2022, Judge Rankin granted the United States's *Application* and issued an *Order* pursuant to 18 U.S.C. § 2703(d) requiring Google to produce certain records (but not content) related to the above-referenced Gmail accounts. (*Id.* (Bates No. 25246–49).) Specifically, the *Order* required Google to produce certain information, including subscriber information, IP and mailing addresses, and header information (but not content). *Id.*

The United States did not renew its preservation request to Google. As a result, the 90-day preservation period that began on October 5, 2022, expired on or about January 3, 2023.

On March 28, 2023, Special Agent Fritz obtained and executed a search warrant related to the three above-referenced email accounts and obtained the contents of those accounts for the period of May 1, 2022, to September 30, 2022. (*See* Bates No. 3203-09.) In response to the Search Warrant, Google provided the requested records on April 4, 2023. Google did not produced preserved records.

2. The T-Mobile Records

The United States did not issue a preservation letter to T-Mobile. However, on October 18, 2022, the United States submitted a § 2703(d) *Application* requesting records from T-Mobile. (Ex. 2 (Bates No. 25251–56.) The T-Mobile § 2703(d) *Application* was similar to the Google 2703(d) *Application*, but included a statement that Miriam Jabotinski also listed a “California phone number ending **1888**” as her contact phone number in the WY Secretary of State filing. On the same day, Judge Rankin issued a § 2703d *Order* to T-Mobile requiring T-Mobile to produce subscriber information for California phone number ending **1888**. (*Id.*) (Bates No. 25257-59.) In response, T-Mobile produced subscriber records revealing that this phone number was subscribed to by Peter Szanto of 11 Shore Pine Dr. in Newport Beach, CA.

C. Defendant’s Motion to Suppress

On February 9, 2024, the Defendant moved to suppress “all evidence from the contents of Defendant’s Internet accounts from Google, and T-Mobile.” (ECF No. 88 at 1.) First, the Defendant argues the issuance of a § 2703(f) preservation request to Google and T-Mobile created an agency relationship with the government, thereby amounting to an unreasonable seizure in violation of the Fourth Amendment. (*Id.* at 1–2, 8–16.) Second, the Defendant asserts that the government’s *Application* for an order under 18 U.S.C. § 2703(d) was not based upon sworn specific and articulable facts. (*Id.* at 16–20.) And third, the Defendant contends that the entire

contents of the internet accounts, and evidence obtained from that data, must be suppressed as fruit of the poisonous tree. (*Id.* at 21–23.)

The Defendant’s arguments are unsupported in fact and law. First, the Defendant has not met his threshold burden of establishing (a) standing or (b) but-for causation that the preservation request was the cause of the government obtaining the contents of his internet account. Second, and alternatively, a preservation request is not a Fourth Amendment search or seizure because it does not create an agency relationship between the government and a service provider. Third, suppression is not an available remedy under § 2703(d), and, if it were, suppression would not be warranted because the § 2703(d) *Order* to Google was supported by reasonable and articulable facts. Finally, even if the preservation request somehow violated the Fourth Amendment, the good-faith exception to the exclusionary rule precludes suppression in this case.

II. Legal Standard and Analysis

As a preliminary matter, a defendant must make threshold showings before he is entitled to an evidentiary hearing. As the Tenth Circuit has summarized:

[A defendant is] required to set forth plainly in his pre-trial motions the grounds upon which he [seeks] relief. To warrant an evidentiary hearing, the motion to suppress must raise factual allegations that are sufficiently definite, specific, detailed, and nonconjectural to enable the court to conclude that contested issues of fact are in issue. A defendant who requests a hearing bears the burden of showing that there are disputed issues of material fact.

United States v. Barajas-Chavez, 358 F.3d 1263, 1266 (10th Cir. 2004) (quotation marks, ellipses, and citations omitted). Federal Rule of Criminal Procedure 47(b) states in part that a party’s “motion must state the grounds on which it is based and the relief or order sought.” Local Criminal Rule 47.1 further states in part that “[a] party who files a motion shall include in the motion a short, concise statement of the arguments and authorities in support of the motion.”

The Stored Communications Act, 18 U.S.C. §§ 2701–2713, regulates access to and disclosure of stored communications and other information held by network service providers. The first three subsections of § 2703 specify procedures that a governmental entity may use to compel a communication service provider to disclose various categories of information pertaining to a subscriber or customer. *See* 18 U.S.C. § 2703(a)–(c). These procedures include search warrants, court orders based on a showing of relevance and materiality (as applicable here), and subpoenas. Section 2703(f) allows a governmental entity to request a service provider to preserve records temporarily. It states that a service provider, “upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.” 18 U.S.C. § 2703(f)(1). The provider is required to retain preserved information for 90 days, and the governmental entity may request a 90-day extension. *See* 18 U.S.C. § 2703(f)(2). After the period of required preservation ends, the provider is free to delete the preserved information. Preservation requests do not apply prospectively: the provider’s duty to preserve is limited to information that the provider already had in its possession when it received the preservation request. Finally, § 2703(f) does not mandate a specific manner of preservation.

The Fourth Amendment protects a citizen’s right “to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” U.S. CONST. AMEND. IV. A search implicating the Fourth Amendment only occurs when “there is actual intrusion into a constitutionally protected area.” *Kyllo v. United States*, 533 U.S. 27, 31 (2001). To determine whether an area is protected by the Fourth Amendment, courts apply a two-part test: 1) “whether the defendant manifested a subjective expectation of privacy in the area searched,” and 2) “whether

society is prepared to recognize that expectation as objectively reasonable.” *United States v. Johnson*, 548 F.3d 995, 999 (10th Cir. 2009).

A. Defendant Fails to Meet his Threshold Burden to Warrant an Evidentiary Hearing.

It is difficult to respond to the Defendant’s Motion to Suppress because the Defendant often lacks precision in his claims,² conflates legal principles, conflates and ignores facts, and, at times, makes inconsistent arguments. Nonetheless, where possible, the government has attempted to determine whether the Defendant has raised any discernable legal objection and responded thereto.

a. Government did not obtain “internet accounts” from T-Mobile.

Initially, the Defendant misstates the facts where he moves to suppress “all evidence from the contents of Defendant’s Internet accounts from Google, and T-Mobile.” ECF No. 88. at 1. The United States did not obtain “internet accounts” from T-Mobile, nor did it issue a preservation letter to T-Mobile. Instead, the United States obtained subscriber information from T-Mobile pursuant to a § 2703(d) *Order*. Further, Defendant has no expectation of privacy in subscriber information. *See, e.g., United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) (“Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment’s privacy expectation) (citations omitted). As

² Defendant does not identify any specific “internet accounts,” but his motion—including the caption—makes clear that he is moving to suppress only the contents of *his* internet account. *See* ECF No. 88 at 2 (“Defendant believes his private messages in his personal internet account were seized” and “Defendant believes that the government ordered copies of the contents of his Internet account”); *Id.* at 8 (referencing the “warrantless preservation of Defendant’s Internet account” and “Google’s and T-Mobile’s acts of preserving Mr. Szanto’s account”). Though not stated, there can be no serious dispute that the personal email account he refers to is **szanto.pp@gmail.com**. And, although the United States’s evidence will show that the Defendant created and controlled Gmail accounts **miriamjabotinski@gmail.com** and **probateestatess@gmail.com** in furtherance of his bankruptcy fraud scheme, these accounts are not the subject of his motion.

such, and as a threshold matter, this Court may summarily dismiss Defendant's argument regarding T-Mobile because the Defendant fails to alleged a factual or legal basis to support his claims.

b. Defendant fails to distinguish between types of Google evidence obtained pursuant to different legal process.

Another difficulty in responding to the Defendant's motion arises from the Defendant's failure to make a distinction between the type of data (non-content) obtained pursuant to the § 2703(d) *Order* issued to Google, and the types of data (non-content and content) obtained pursuant to the Google search warrant. For instance, he claims he "believes his private messages in his personal internet account were seized" pursuant to 18 U.S.C. § 2703(d).³ ECF No. 88 at 2. Even a cursory review of discovery reveals the contents of his emails were obtained by way of a search warrant and not pursuant to 18 U.S.C. § 2703(d).⁴ This is important because, as it relates to the § 2703(d) *Order*, Defendant has no standing under the Fourth Amendment to seek suppression of non-content records because he has no reasonable expectation of privacy in any non-content records, including subscriber information, IP addresses, or email to/from data (header information) that was produced to the government.

As a result, and as a threshold matter, there is no basis for suppression of any non-content materials. The Supreme Court has made clear that individuals retain no reasonable expectation of privacy in information revealed to third parties, even if they have a subjective expectation that the third parties will keep the information confidential. *See, e.g., United States v. Miller*, 425 U.S. 435, 443 (1976) (bank records); *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979) (dialed telephone numbers); *contra Carpenter v. United States*, 585 U.S. 296 (2018) (finding privacy interest in cell

³ He later claims "[a]t some point in time after the preservation date, the government obtained an order under 18 U.S.C. § 2703(d) to justify the account's seizure and subsequent search. *Id.* at 7. Again, this is factually inaccurate.

⁴ Indeed, Defendant only makes a single passing reference to "search warrants" [sic] in his motion, falling far short of the threshold requirements for triggering an evidentiary hearing.

site location information amassed by third party service providers over an extended period). “[A] defendant ‘has no expectation of privacy in IP addresses’ or basic subscriber information because internet users ‘should know that this information is provided to and used by Internet service providers for the specific purpose of directing and routing information.’” *United States v. Rosenow*, 50 F.4th 715, 738 (9th Cir. 2022) (quoting *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008)); *see also United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010) (no expectation of privacy in subscriber information because it is “voluntarily conveyed” to a third party); *United States v. Wellbeloved-Stone*, 777 Fed. App’x 605 (4th Cir. 2019) (holding “no reasonable expectation of privacy in [defendant’s] IP address or subscriber information”); *United States v. Ulbricht*, 858 F.3d 71, 97 (2d Cir. 2017) (*abrogated* on other grounds) (holding that a warrant is not necessary to collect IP address information, for which there is not a legitimate privacy interest); *United States v. Caira*, 833 F.3d 803, 806 (7th Cir. 2016) (holding that the defendant did not have a reasonable expectation of privacy in his IP addresses). Similarly, individuals have no expectation of privacy in the to/from lines of emails (header information) that are provided in response to a § 2703(d) order: this information is analogous to the “information people put on the outside of an envelope” which is “voluntarily transmitted to third parties,” therefore obliterating any privacy expectation. *Rosenow*, 50 F.4th at 738. Because the Defendant has no privacy expectation in the non-content data, there can be no Fourth Amendment violation (and no “fruit of the poisonous tree” argument). Suppression is not available as to these records.

- c. Defendant’s “beliefs” and “assumptions” are insufficient to meet his threshold burden and Defendant cannot show “but-for” causality to warrant suppression.

The Defendant’s motion is replete with “beliefs” and “assumptions” that are insufficient to meet his threshold burden to warrant an evidentiary hearing as it relates to the argument that “preservation is a Fourth Amendment seizure.” (ECF No. 88 at 11.) Defendant complains that he

“is forced to assume” the existence of preservation letters, *see id.* at 2 n.1, and that he “is unaware of whether preservation occurred.” *See id.* at 6. However, as outlined above, the government’s discovery makes clear that a preservation letter was sent to Google on October 5, 2022 and the § 2703(d) order issued to Google is dated October 6, 2022. Given these undisputed facts, and even assuming, *arguendo*, that a preservation request by itself amounts to a Fourth Amendment seizure, the Defendant has not shown a factual basis to support the necessary conclusion that the United States obtained the § 2703(d) information (or the Search Warrant results) as a direct result of the preservation request. As mentioned, any alleged seizure of data expired on January 3, 2023, well before Judge Rankin authorized a search warrant of the accounts on March 23, 2023. As such, at the time the warrant was executed some 2 and ½ months later, the 90-day period for preservation had expired. The Defendant has offered nothing to support his claim that the request for preservation had any impact on the information ultimately produced to the government. Indeed, the facts are too the contrary. Because “but-for causality is . . . [a] necessary . . . condition for suppression,” *Hudson v. Michigan*, 547 U.S. 586, 592 (2006), the Defendant’s cannot meet his threshold burden. *See also United States v. Rosenow*, 50 F.4th 715, 736 (9th Cir. 2022) (assuming preservation implicated the Fourth Amendment and finding no basis for suppression where defendant failed to establish the preservation request was “but-for” cause of the government obtaining the challenged evidence); *United States v. Zwiefelhofer*, 2023 WL 4931899, at *2 (M.D. Fla. Aug. 2, 2023) (relying on *Rosenow* and declining to address constitutionality of § 2703(f) where defendant “offers no evidence that the information he wants suppressed came from the preservation letters”). Thus, his motion to suppress must fail and the Court need not address his remaining arguments.

B. Alternatively, preservation does not create an agency relationship, and thus does not implicate the Fourth Amendment.

This Court need not address the Defendant’s claim that the preservation request to Google implicates the Fourth Amendment because even assuming it does, as illustrated above, the Defendant has failed to establish a basis for suppression. Nonetheless, and in the alternative, the United States disposes of Defendant’s arguments below.

The Defendant argues that the simple act of the government requesting Google to preserve his Gmail account was “Fourth Amendment state action,” effectively making Google an agent for the government. (ECF No. 88 at 8.) But the Fourth Amendment does not extend to conduct by a private individual not acting as an agent of the government. *See United States v. Jacobsen*, 466 U.S. 109, 113 (1984). When a business complies with a legal duty to preserve information in its possession, it does not become a government agent. For example, all taxpayers are required to keep tax records, *see* 26 U.S.C. § 6001, but such a requirement does not transform all taxpayers into government agents. Nor does 18 U.S.C. § 1519, which criminalizes knowingly destroying records with intent to obstruct a federal investigation, convert everyone in possession of such records into government agents.

The Supreme Court has come to the same conclusion in a similar context. In *California Bankers Ass’n v. Shultz*, 416 U.S. 21 (1974), the Supreme Court considered constitutional challenges to the Bank Secrecy Act and associated regulations that required banks to keep certain records (for years) and required banks to make certain reports useful in criminal investigations of its customers. *Id.* at 26 (citing 12 U.S.C. § 1829b(g)). Banks argued that the Act was unconstitutional because it made “the banks the agents of the Government in surveillance of its citizens.” *Id.* at 45. The Supreme Court summarily dismissed this argument, explaining that “[s]uch recordkeeping requirements are scarcely a novelty.” *Id.* at 45-46 (noting that “this Court has been

faced with numerous case involving similar recordkeeping requirements”). The Supreme Court went onto find that “the mere maintenance of the records by the banks under compulsion of the regulations” does not constitute a seizure or seizure under the Fourth Amendment. *Id.* at 54. A similar finding that preservation request is neither a search nor seizure is warranted here, where the preservation requirement of § 2703(f) is analogous to the Bank Secrecy Act requirements at issue in *California Bankers Ass’n* that required banks to maintain copies of certain records for a period of time, only to be subject to disclosure to the government in the event the government obtains further legal process.

In support of his argument, the Defendant relies on inapposite case law. *See Coolidge v. New Hampshire*, 403 U.S. 443 (analyzing the automobile exception to a search warrant requirement in the context of evidence admitted during a murder trial); *Skinner v. Railway Labor Executives’ Assn.*, 489 U.S. 602 (analyzing whether alcohol and drug tests were intrusive in the context of the Federal Railroad Safety Act); *Commonwealth v. Gumkowski*, 167 N.E.3d 803 (Mass. 2021) (analyzing whether cell site location information was improperly disclosed by a service provider under 18 U.S.C. § 2702 rather than § 2703); and *United States v. Hardin*, 539 F.3d 404 (2008) (analyzing whether law enforcement erred in executing a search warrant for a defendant at an apartment in which he was staying at a guest based upon information gathered from an apartment manager). However, these cases are distinguished here because the underlying facts involved notably different government or law enforcement conduct and have no relation to the preservation request challenged by the Defendant.

Moreover, even if the mere act of requesting a 90-day preservation of account information could create an agency relationship between the government and a service provider, that agency relationship would not extend beyond the statutorily mandated preservation period. Here, the 90-

day preservation period expired on or about January 3, 2023, well before Special Agent Fritz obtained a search warrant for the contents of the three Gmail accounts, including Defendant's Gmail account.

a. A preservation request is not a Fourth Amendment search or seizure.

The Defendant alleges that the mere act of sending a letter requesting preservation amounts to a seizure under the Fourth Amendment. Such a claim is without support of fact or law. When the government sends a preservation request to a service provider, it obtains no information at all, and the account owner retains full and unhindered access to his account. It therefore is not a seizure, which requires "some meaningful interference with an individual's possessory interests in that property." *United States v. Jefferson*, 566 F.3d 928, 933 (9th Cir. 2009) (quoting *Jacobsen*, 466 U.S. at 113). In addition, § 2703(f) includes no general recordkeeping requirements; a § 2703(f) request requires only temporary preservation of information that the provider has already chosen to store. This temporary mandate does not constitute a meaningful interference with an account holder's possessory interests.

Nor is preservation a Fourth Amendment search. The government conducts a Fourth Amendment search in two circumstances. First, the government conducts a search when it "infringes 'an expectation of privacy that society is prepared to consider reasonable.'" *United States v. Lundin*, 817 F.3d 1151, 1158 (9th Cir. 2016) (quoting *Jacobsen*, 466 U.S. at 113). A preservation request infringes no privacy interest: the government obtains no information, and the service provider merely retains information it already stores.

Second, the government conducts a search when it "physically occupie[s] private property for the purpose of obtaining information." *United States v. Jones*, 565 U.S. 400, 404 (2012). To constitute a search under *Jones*, the invasion of private property must constitute a trespass. *See*

Jones, 565 U.S. at 411–13. A preservation request cannot constitute a search under *Jones* for multiple reasons because the government does not receive information or occupy private property as a result.

The Defendant claims that “[p]reservation of his account caused a Fourth Amendment seizure because it dispossessed him of control over the account.” ECF No. 88 at 11. To the contrary, no aspect of the preservation process changed the amount of control the Defendant had over his accounts. First, even if a service provider generates a copy that is “then stored outside the user’s control so the user cannot alter or delete any files,” the end user responsible for the initial creation of that data has not been dispossessed of any objective form of control. (*Id.* at 11–12.)

Significantly, Defendant fails to cite any case holding that a preservation mandate constitutes a seizure or a search. In fact, the only court that appears to have specifically addressed the issue, has held that preservation letters do not amount to a Fourth Amendment search or seizure. Specifically, in *United States v. Rosenow*, No. 17-cr-3430, 2018 WL 6064949, at *10 (S.D. Cal. Nov. 20, 2018), the court found that preservation requests “did not interfere with the Defendant’s use of his accounts and did not entitle the Government to obtain any information without further legal process.” The court concluded that the requests “did not amount to an intrusion subject to Fourth Amendment requirements.”⁵ *Id.*

When the government sends a preservation request to a service provider, it obtains no information at all, and the account owner retains full and unhindered access to his account. It therefore is not a seizure, which requires “some meaningful interference with an individual’s

⁵ On appeal, the Ninth Circuit declined to address the issue as to whether preservation requests constitute a Fourth Amendment violation. Rather, the Court held “even assuming that they do, there is no basis for suppression” because the Defendant failed to establish the preservation request was a “but-for” cause of the government obtaining the challenged evidence. *United States v. Rosenow*, 50 F.4th 715, 736 (9th Cir. 2022).

possessory interests in that property.” *Jacobsen*, 466 U.S. at 113. In addition, § 2703(f) includes no general recordkeeping requirements. Rather, a § 2703(f) request requires only temporary preservation of information that the provider has already chosen to store. This temporary mandate does not constitute a meaningful interference with an account holder’s possessory interests. Even in the absence of a preservation request, an end user has no discretion as to the data storage methods utilized by a given service provider. That is, despite any deletion or alteration of an account’s contents on the user end, an internet service provider may generate backups of the unaltered data throughout the ordinary course of business, even if such backups are retained only for a short period.

Even if preservation of the Defendants accounts amounted to a search or seizure, it would not violate the Fourth Amendment because Google had authority to create copies of the Defendant’s digital account information, and the Defendant consented to it. It is well settled that consent is an exception to the Fourth Amendment’s warrant requirement. *See Schneekloth v. Bustamonte*, 412 U.S. 218, 219 (1973). Moreover, the search or seizure can be authorized by “a third party who possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected.” *United States v. Matlock*, 415 U.S. 164, 171 (1974).

Here, Google had a sufficient relationship to the Defendant’s Gmail account to preserve or copy its contents. Indeed, copying and storage are the basic functions of the service Google provided the Defendant. *See Hatley v. Watts*, 917 F.3d 770, 791–92 (4th Cir. 2019) (“when a web-based email service receives an email, it typically generates numerous copies of the email”). Moreover, a service provider’s terms of service can establish subscriber consent. *See, e.g., United States v. Adkinson*, 916 F.3d 605, 610 (7th Cir. 2019) (rejecting Fourth Amendment challenge to disclosure of cell phone location information in part because defendant “agreed to T-Mobile’s

policy that T-Mobile could disclose information when reasonably necessary to protect its rights, interests, property, or safety”). Here, Google customers like the Defendant accept and agree to be bound by the terms and conditions of those services.⁶ Indeed, the terms of service providers like Google dictate that the providers may access, preserve, and disclose account information under a variety of circumstances. Because the defendant consented to Google’s preservation policies through creating and maintaining his account, such preservation does not violate the Fourth Amendment. In short, Google had authority to copy Defendant’s email account and he consented to the preservation.

C. Suppression is not a remedy for violations of § 2703(d).

Defendant complains that the United States’ § 2703(d) *Application* fails to alleged “specific and articulable facts” as required under § 2703(d). As a threshold matter, however, even assuming, *arguendo*, the government’s *Application* is facially deficient, suppression is not a remedy. *United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008) (“violations of ECPA [including 2703(d)] do not warrant exclusion of evidence”)(citations omitted).

Nonetheless, though the Court need not decide the issue, even a cursory review of the government’s § 2703(d) *Application* belies Defendant claims that it is based on “inarticulate hunches and possibilities rather than an objective standard because the creation of a corporation and the mere filing of a bankruptcy – both perfectly legal activities in themselves” does not satisfy this *Terry* standard.⁷ *Id.* at 17. However, a plain reading of the *Application* establishes much more

⁶ See Google Privacy & Terms, <https://policies.google.com/privacy?hl=en-US>.

⁷ The Defendant also complains that the government’s § 2703(d) *Application* lacks “probable cause” and was not “sworn,” but goes on to recognize there are no such requirements under § 2703(d) which “parallels the standard established” in *Terry v. Ohio*. (See ECF 88 at 16.) Indeed, as Defendant concedes, the standard of proof supporting a Court’s issuance of a § 2703(d) order is based upon the government’s stating “specific and articulable facts showing that there were reasonable grounds to believe . . . the records or other information sought, are relevant and

than the innocent creation of a Wyoming corporation and the filing of a bankruptcy in Wyoming, as the Defendant disingenuously implies. *Id.* Rather, the government outlined “specific and articulable facts” showing the Gmail accounts at issue are relevant and material to the United States’s investigation of the Defendant’s pattern of conduct in thwarting the lawful foreclosure of his California home through the serial filing of bankruptcy petitions in several jurisdictions over a nine-year period.

Further, Defendant ignores the specific dates and facts outlined in the government’s § 2703(d) *Application* reflecting a pattern of bankruptcy fraud. The Defendant also ignores a reference to the finding of a U.S. Bankruptcy Chief Judge Christopher Latham in the Southern District of California, who quickly dismissed Defendant’s bankruptcy petition for a lack of venue (thereby calling into question Defendant’s bankruptcy filings in Nevada and Oregon). The Defendant further ignores the specific and articulable facts of Judge Latham’s dismissal and lifting the automatic stay, based on a finding that the Defendant had acted in “bad faith” and “engaged in a scheme to delay and hinder [JP Morgan Chase’s] effort to foreclose” on his California home. And the Defendant ignores the specific and articulable facts of his filing of a Chapter 11 bankruptcy in Wyoming on July 12, 2022, upon the heels of Judge Latham’s findings, under what are unquestionably suspect circumstances indicative of fraud. Given the lesser standard that applies to a § 2703(d) *Application*, the United States’ § 2703(d) *Application* was more than sufficient to satisfy § 2703(d).

material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d); *see also United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008) (noting that “the ‘specific and articulable facts’ standard derives from the Supreme Court’s decision in *Terry*”).

D. The good faith exception precludes suppression.

Defendant argues the evidence obtained from the Defendant's internet account must be suppressed as fruit of the poisonous tree. In doing so, the Defendant claims that "the government had access to that preserved copy as a result of its prior constitutional violation," and on that basis, "the entire contents of Defendant's accounts must be suppressed." *Id.* This claim is unsupported by any facts. The government did not take possession of the Defendant's account data at the time the preservation requests were issued, the government did not obtain a "preserved" copy in response to the Search Warrant, and the government cannot therefore be fairly characterized as having had "access" to the content of Defendant's internet account through the preservation request. His failure to allege any facts as to why the information obtained pursuant to a Search Warrant must be suppressed as "fruit of the poisonous tree," requires this Court to summarily reject his challenge.

Alternatively, even if the preservation in this case violated the Fourth Amendment, suppression would not be an appropriate remedy. In *Illinois v. Krull*, 480 U.S. 340, 349–50 (1987), the Supreme Court held that the good-faith exception to the exclusionary rule applies where law enforcement reasonably relies on a statute later determined to be unconstitutional. *See also United States v. Korte*, 918 F.3d 750, 757–59 (9th Cir. 2019) (applying *Krull* to reject suppression of cell-site information obtained in good-faith reliance on 18 U.S.C. § 2703(d)); *United States v. Warshak*, 631 F.3d 266, 288–92 (6th Cir. 2010) (holding that government relied in good faith on 18 U.S.C. § 2703 in compelling disclosure of email content with a subpoena and court order).

Moreover, this Court may conclude that law enforcement relied in good faith on a statute without resolving the statute's constitutionality. *See, e.g., United States v. Vanness*, 342 F.3d 1093, 1098 (10th Cir. 2003). Despite the Defendant's argument to the contrary, *Krull* applies here because the United States followed § 2703(f) when it sent a preservation request to Google, and

because it appears that no court has ever found this provision unconstitutional. And even if the United States had not obtained legal process to the service providers within the 90-day preservation period, nothing in § 2703(f) sets a deadline for the government to seek legal process. (ECF No. 88 at 21.) Instead, § 2703(f) only requires providers to maintain stored information for a limited period, after which the provider is free to delete any preserved information. Because the United States reasonably relied on the procedures of § 2703, *Krull* precludes suppression of the Defendant's account data.

III. Conclusion

For the foregoing reasons, this Court should summarily deny the Defendant's Motion to Suppress Data Obtained From Defendant's Internet Accounts without an evidentiary hearing.

DATED this 7th day of March 2024.

Respectfully submitted,

NICHOLAS VASSALLO
United States Attorney

By: /s/ Margaret M. Vierbuchen
MARGARET M. VIERBUCHEN
Assistant United States Attorney

CERTIFICATE OF SERVICE

This is to certify that on the 7th day of March 2024, I served a true and correct copy of the foregoing document upon counsel of record for the Defendant via CM/ECF.

/s/ Amanda R. Hudson

UNITED STATES ATTORNEY'S OFFICE